Amendments to the Specification

On page 5, please amend the paragraph at lines 21-23 by replacing it with the following replacement paragraph:

A BIOS (Basic Input Output System) may be provided within the monitoring component itself. By providing the BIOS file within the monitoring component, the BIOS file may be inherently trusted.

On pages 27-28, please replace the paragraph beginning at line 5 of page 27 with the following replacement paragraph:

Referring to Fig. 8, herein, there is illustrated schematically a use model followed by a user of the computer entity navigating through one or more states. In step 800, after turning on a power supply to the computing entity, the computer boots up via the BIOS program. The boot process is very similar to re-booting the computer from an existing state. In each case, control of microprocessor 201 is seized by the BIOS component 301. The trusted component 202 measures a set of integrity metric signals from the BIOS 301, to determine a status of the BIOS 301. In step 801, the graphical user interface displays a menu option for entry into a plurality of different states. One of the states displayed on the menu is a trusted state as described herein before. The user manually selects a state in which to enter by using the keyboard or pointing device of the graphical user interface, for example by clicking a pointer icon over a state icon displayed on the graphical user interface. Alternatively, an automatic selection of a state may be made by a smartcard or via a network connection from state selection options generated by the BIOS. After selection of a state, the BIOS loads a program which loads a selected operating system corresponding with the state. A different load program is used for each of the plurality of different possible states. The trusted component measures that program in broadly a similar way to the way in which it measures the BIOS, so that the trusted component can record and determine which state has been loaded. When an external entity requests that the trusted

component supplies integrity metrics, the trusted component supplies both the BIOS metrics and the loaded program metrics. In step 802, the computing entity enters the selected state. Once in the selected state, in step 803 the user has access to a set of physical and logical resources in that state. For example, in a relatively insecure state, the user may have full internet access through a modem device comprising the computing entity, may have full access to one or a plurality of hard disk drives or CD readers/writers, and may have full access to a floppy disk drive, as well as having access to a plurality of pre-loaded commercially available applications programs. On the other hand, if the user selects a trusted state having a relatively high level of trust, in that state the user may have available a single operating system, a limited set of applications, for example a word processor, accounts package, or data base, and use of a printer device, but in that state, use of a hard disk drive, a floppy disk drive, or the internet may be restricted. Each selection of a separate state into which the computer may be booted may be pre-configured by configuration of the BIOS component 301. A choice of states is presented by the BIOS to a user. Once a state is selected, the BIOS cause the selected state to load by calling up an operating system loading program to load that state. The states themselves are pre-configured by the loading and the relevant operating system. For entry into trusted states, entry into those states is via operation of the BIOS component 301, and including monitoring by the trusted component in monitoring process 706. In order to enter a trusted state, a user must boot or e-boot the computer platform in step 804. Similarly, to exit from a trusted state, the user must also boot or re-boot the computing entity in step 804. To navigate from a state having a lower trust level, for example the second state(701), or the third state (702), the user may navigate from that state to another state in step 805, which, in the best mode involves re-booting of the computing entity via the BIOS.